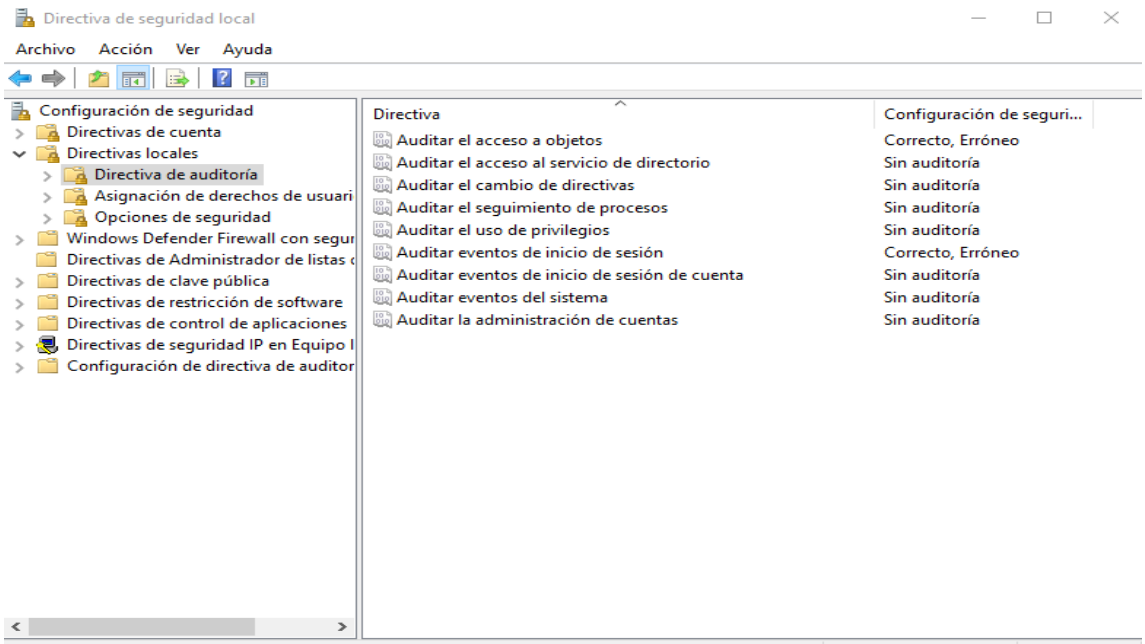
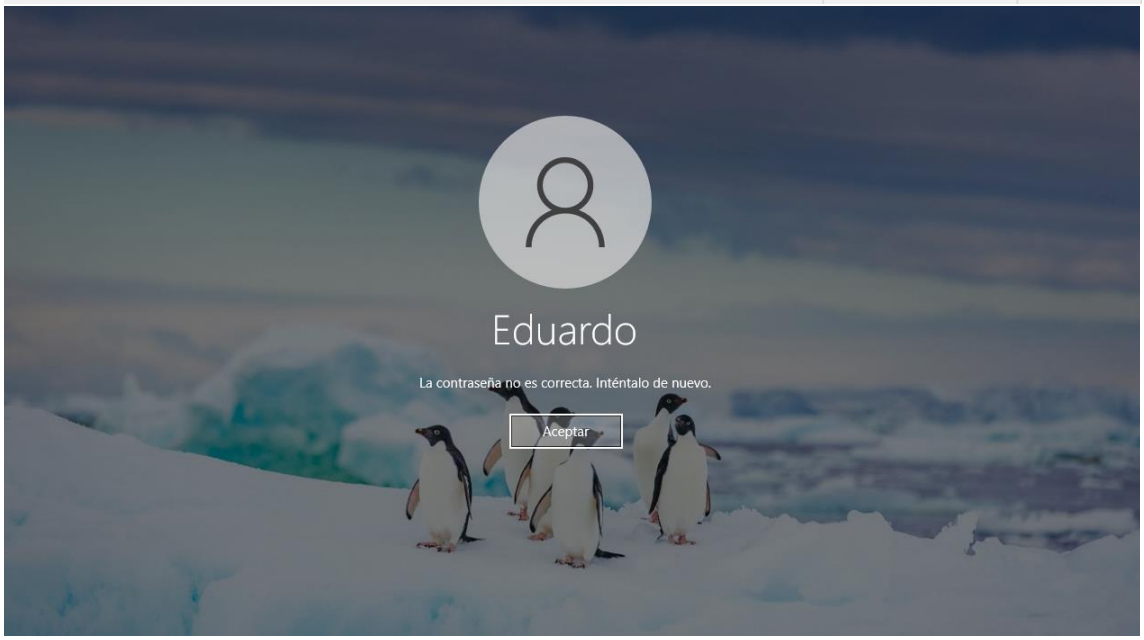
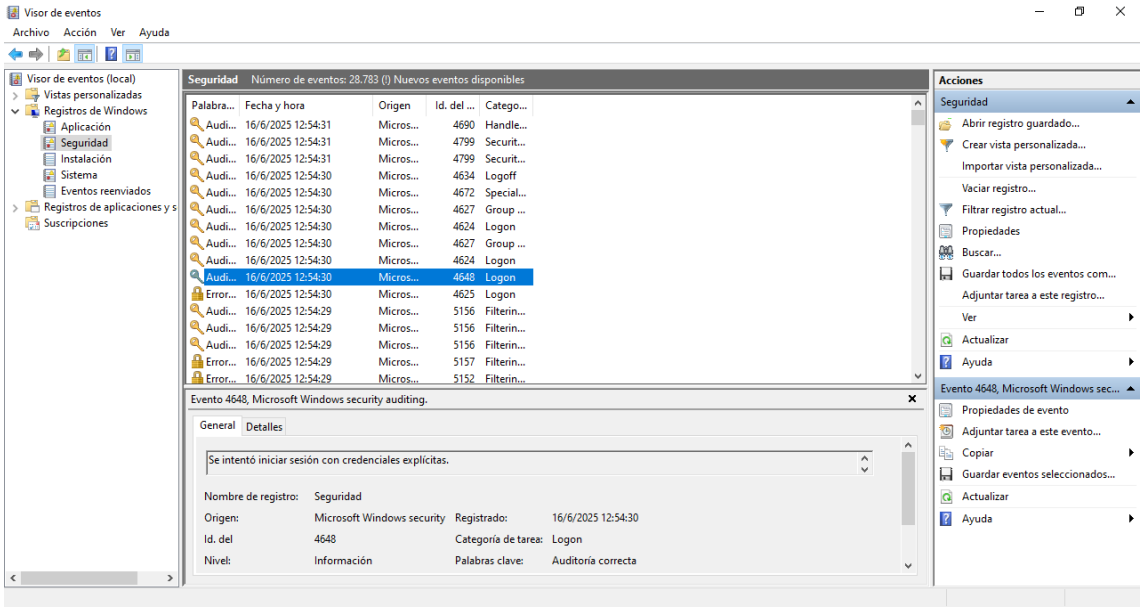
Laboratorio 4: Seguridad del Sistema

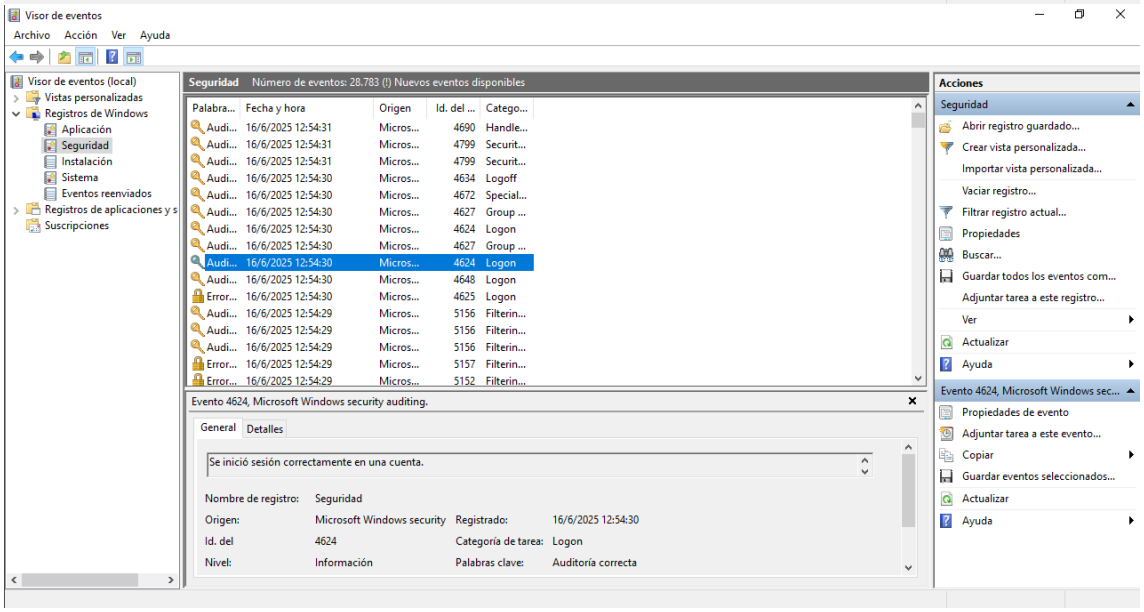
Auditoría de Seguridad

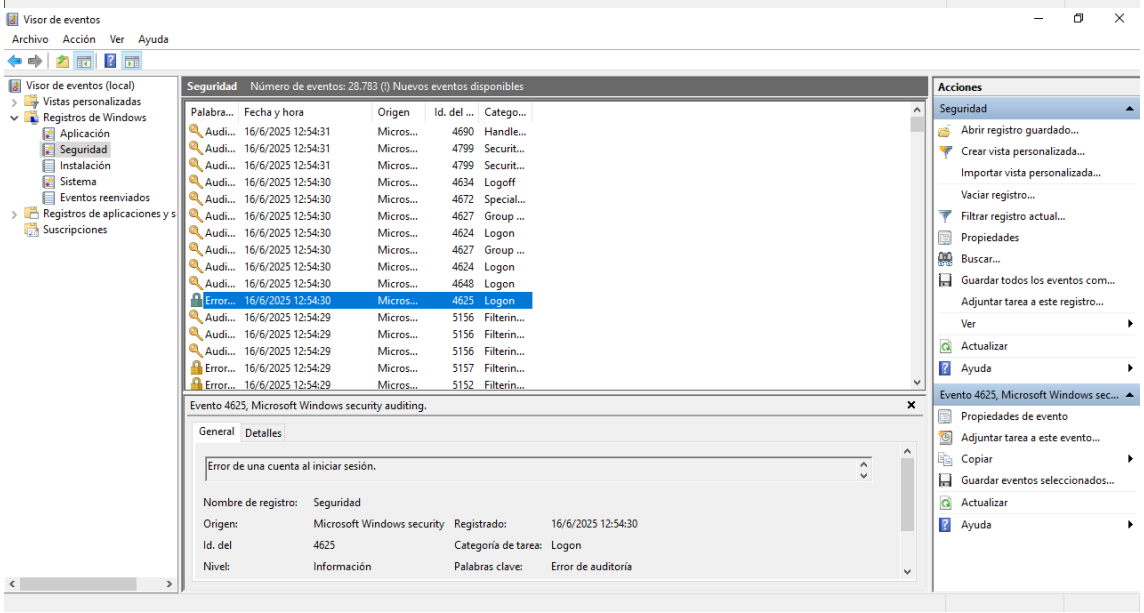
Se activaron los logs de seguridad en el sistema operativo Windows para registrar eventos importantes como intentos de inicio de sesión fallidos y accesos denegados. Para validar su funcionamiento, se simularon estos eventos y se accedió al Visor de eventos para analizar los logs generados.






Visor de eventos
Archivo Acción Ver Ayuda
Visor de eventos (local)
Vistas personalizadas
Registros de Windows
Aplicación
Seguridad
Instalación
Sistema
Eventos reenviados
Registros de aplicaciones y s
Suscripciones
Seguridad Número de eventos: 28.783 (!) Nuevos eventos disponibles
Palabra... Fecha y hora Origen Id. del ... Catego...
Audi... 16/6/2025 12:54:31 Micros... 4690 Handle...
Audi... 16/6/2025 12:54:31 Micros... 4799 Securit...
Audi... 16/6/2025 12:54:31 Micros... 4799 Securit...
Audi... 16/6/2025 12:54:30 Micros... 4634 Logoff
Audi... 16/6/2025 12:54:30 Micros... 4672 Special...
Audi... 16/6/2025 12:54:30 Micros... 4627 Group ...
Audi... 16/6/2025 12:54:30 Micros... 4624 Logon
Audi... 16/6/2025 12:54:30 Micros... 4627 Group ...
Audi... 16/6/2025 12:54:30 Micros... 4624 Logon
Audi... 16/6/2025 12:54:30 Micros... 4648 Logon
Error... 16/6/2025 12:54:30 Micros... 4625 Logon
Audi... 16/6/2025 12:54:29 Micros... 5156 Filterin...
Audi... 16/6/2025 12:54:29 Micros... 5156 Filterin...
Audi... 16/6/2025 12:54:29 Micros... 5156 Filterin...
Error... 16/6/2025 12:54:29 Micros... 5157 Filterin...
Error... 16/6/2025 12:54:29 Micros... 5152 Filterin...
Evento 4648, Microsoft Windows security auditing.
General Detalles
Se intentó iniciar sesión con credenciales explícitas.
Nombre de registro: Seguridad
Origen: Microsoft Windows security Registrado: 16/6/2025 12:54:30
Id. del 4648 Categoría de tarea: Logon
Nivel: Información Palabras clave: Auditoría correcta
Acciones
Seguridad
Abrir registro guardado...
Crear vista personalizada...
Importar vista personalizada...
Vaciar registro...
Filtrar registro actual...
Propiedades
Buscar...
Guardar todos los eventos com...
Adjuntar tarea a este registro...
Ver
Actualizar
Ayuda
Evento 4648, Microsoft Windows sec...
Propiedades de evento
Adjuntar tarea a este evento...
Copiar
Guardar eventos seleccionados...
Actualizar
Ayuda


Visor de eventos
Archivo Acción Ver Ayuda
Visor de eventos (local)
Vistas personalizadas
Registros de Windows
Aplicación
Seguridad
Instalación
Sistema
Eventos reenviados
Registros de aplicaciones y s
Suscripciones
Seguridad Número de eventos: 28.783 (!) Nuevos eventos disponibles
Palabra... Fecha y hora Origen Id. del ... Catego...
Audi... 16/6/2025 12:54:31 Micros... 4690 Handle...
Audi... 16/6/2025 12:54:31 Micros... 4799 Securit...
Audi... 16/6/2025 12:54:31 Micros... 4799 Securit...
Audi... 16/6/2025 12:54:30 Micros... 4634 Logoff
Audi... 16/6/2025 12:54:30 Micros... 4672 Special...
Audi... 16/6/2025 12:54:30 Micros... 4627 Group ...
Audi... 16/6/2025 12:54:30 Micros... 4624 Logon
Audi... 16/6/2025 12:54:30 Micros... 4627 Group ...
Audi... 16/6/2025 12:54:30 Micros... 4624 Logon
Audi... 16/6/2025 12:54:30 Micros... 4648 Logon
Error... 16/6/2025 12:54:30 Micros... 4625 Logon
Audi... 16/6/2025 12:54:29 Micros... 5156 Filterin...
Audi... 16/6/2025 12:54:29 Micros... 5156 Filterin...
Audi... 16/6/2025 12:54:29 Micros... 5156 Filterin...
Error... 16/6/2025 12:54:29 Micros... 5157 Filterin...
Error... 16/6/2025 12:54:29 Micros... 5152 Filterin...
Evento 4624, Microsoft Windows security auditing.
General Detalles
Se inició sesión correctamente en una cuenta.
Nombre de registro: Seguridad
Origen: Microsoft Windows security Registrado: 16/6/2025 12:54:30
Id. del 4624 Categoría de tarea: Logon
Nivel: Información Palabras clave: Auditoría correcta
Acciones
Seguridad
Abrir registro guardado...
Crear vista personalizada...
Importar vista personalizada...
Vaciar registro...
Filtrar registro actual...
Propiedades
Buscar...
Guardar todos los eventos com...
Adjuntar tarea a este registro...
Ver
Actualizar
Ayuda
Evento 4624, Microsoft Windows sec...
Propiedades de evento
Adjuntar tarea a este evento...
Copiar
Guardar eventos seleccionados...
Actualizar
Ayuda


Visor de eventos
Archivo Acción Ver Ayuda
Visor de eventos (local)
Vistas personalizadas
Registros de Windows
Aplicación
Seguridad
Instalación
Sistema
Eventos reenviados
Registros de aplicaciones y s
Suscripciones
Seguridad Número de eventos: 28.783 (!) Nuevos eventos disponibles
Palabra... Fecha y hora Origen Id. del ... Catego...
Audi... 16/6/2025 12:54:31 Micros... 4690 Handle...
Audi... 16/6/2025 12:54:31 Micros... 4799 Securit...
Audi... 16/6/2025 12:54:31 Micros... 4799 Securit...
Audi... 16/6/2025 12:54:30 Micros... 4634 Logoff
Audi... 16/6/2025 12:54:30 Micros... 4672 Special...
Audi... 16/6/2025 12:54:30 Micros... 4627 Group ...
Audi... 16/6/2025 12:54:30 Micros... 4624 Logon
Audi... 16/6/2025 12:54:30 Micros... 4627 Group ...
Audi... 16/6/2025 12:54:30 Micros... 4624 Logon
Audi... 16/6/2025 12:54:30 Micros... 4648 Logon
Error... 16/6/2025 12:54:30 Micros... 4625 Logon
Audi... 16/6/2025 12:54:29 Micros... 5156 Filterin...
Audi... 16/6/2025 12:54:29 Micros... 5156 Filterin...
Audi... 16/6/2025 12:54:29 Micros... 5156 Filterin...
Error... 16/6/2025 12:54:29 Micros... 5157 Filterin...
Error... 16/6/2025 12:54:29 Micros... 5152 Filterin...
Evento 4625, Microsoft Windows security auditing.
General Detalles
Error de una cuenta al iniciar sesión.
Nombre de registro: Seguridad
Origen: Microsoft Windows security Registrado: 16/6/2025 12:54:30
Id. del 4625 Categoría de tarea: Logon
Nivel: Información Palabras clave: Error de auditoría
Acciones
Seguridad
Abrir registro guardado...
Crear vista personalizada...
Importar vista personalizada...
Vaciar registro...
Filtrar registro actual...
Propiedades
Buscar...
Guardar todos los eventos com...
Adjuntar tarea a este registro...
Ver
Actualizar
Ayuda
Evento 4625, Microsoft Windows sec...
Propiedades de evento
Adjuntar tarea a este evento...
Copiar
Guardar eventos seleccionados...
Actualizar
Ayuda

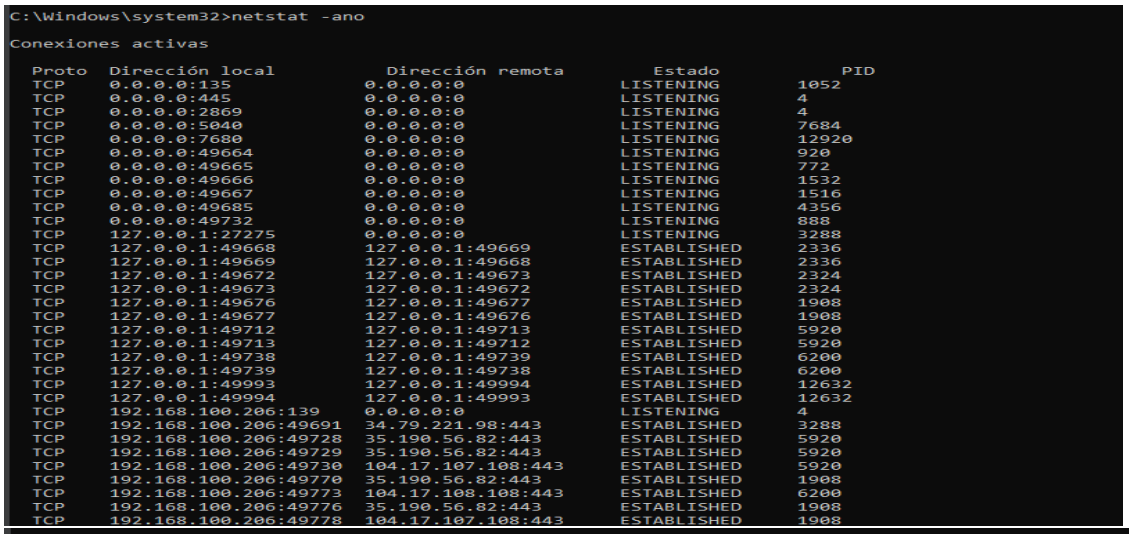
Análisis de Vulnerabilidades

Se realizó un escaneo básico del sistema para identificar posibles vulnerabilidades. Durante este análisis se detectaron varios servicios activos que, en el contexto actual, no resultan necesarios y podrían representar un riesgo o consumir recursos innecesariamente. Entre estos servicios se documentan:

- **Servicio de Telefonía (Telephony Service):** No se utiliza telefonía en el equipo, por lo que este servicio está innecesariamente activo.
- **WalletService:** Relacionado con funcionalidades de billeteras digitales, no utilizadas en este equipo.
- **Servicios telefónicos adicionales:** Incluyen procesos y servicios que no aportan a la función actual del equipo.

La desactivación de estos servicios podría contribuir a mejorar la seguridad y el rendimiento del sistema, al reducir la superficie de ataque y liberar recursos.

Además, se verificó que el sistema está completamente actualizado a través de Windows Update, eliminando vulnerabilidades conocidas que se corrigen mediante actualizaciones oficiales.



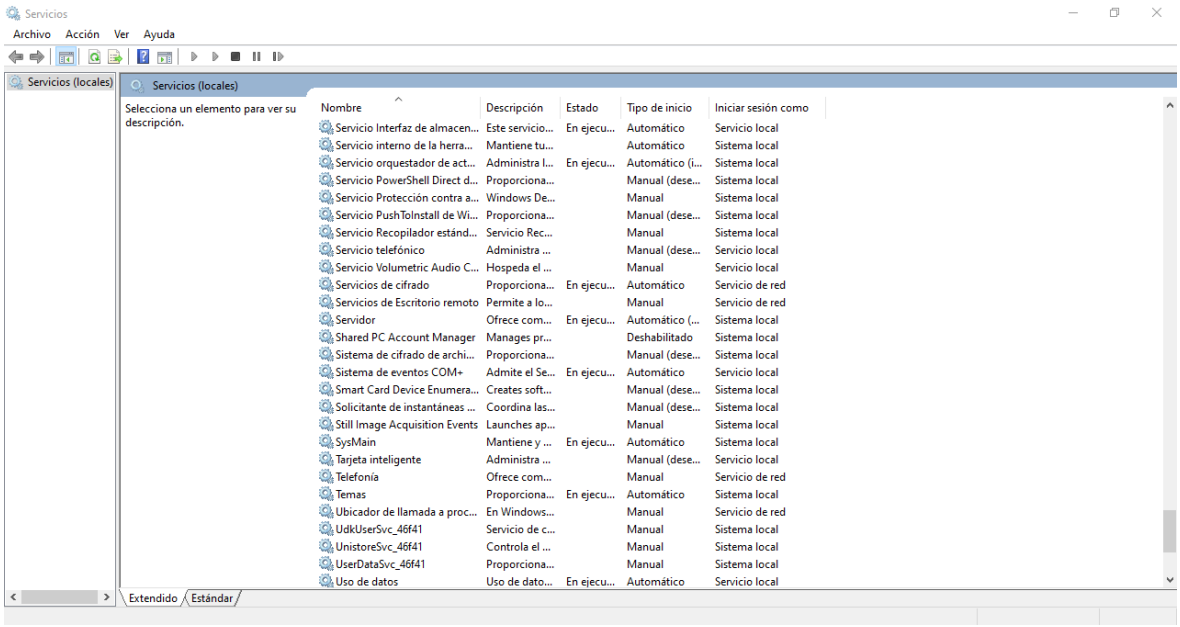
```
C:\Windows\system32>netstat -ano

Conexiones activas

  Proto  Dirección local          Dirección remota        Estado           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1052
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       7684
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       12920
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       920
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       772
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1532
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1516
  TCP    0.0.0.0:49685          0.0.0.0:0              LISTENING       4356
  TCP    0.0.0.0:49732          0.0.0.0:0              LISTENING       888
  TCP    127.0.0.1:27275        0.0.0.0:0              LISTENING       3288
  TCP    127.0.0.1:49668        127.0.0.1:49669        ESTABLISHED     2336
  TCP    127.0.0.1:49669        127.0.0.1:49668        ESTABLISHED     2336
  TCP    127.0.0.1:49672        127.0.0.1:49673        ESTABLISHED     2324
  TCP    127.0.0.1:49673        127.0.0.1:49672        ESTABLISHED     2324
  TCP    127.0.0.1:49676        127.0.0.1:49677        ESTABLISHED     1908
  TCP    127.0.0.1:49677        127.0.0.1:49676        ESTABLISHED     1908
  TCP    127.0.0.1:49712        127.0.0.1:49713        ESTABLISHED     5920
  TCP    127.0.0.1:49713        127.0.0.1:49712        ESTABLISHED     5920
  TCP    127.0.0.1:49738        127.0.0.1:49739        ESTABLISHED     6200
  TCP    127.0.0.1:49739        127.0.0.1:49738        ESTABLISHED     6200
  TCP    127.0.0.1:49993        127.0.0.1:49994        ESTABLISHED     12632
  TCP    127.0.0.1:49994        127.0.0.1:49993        ESTABLISHED     12632
  TCP    192.168.100.206:139    0.0.0.0:0              LISTENING       4
  TCP    192.168.100.206:49691  34.79.221.98:443       ESTABLISHED     3288
  TCP    192.168.100.206:49728  35.190.56.82:443       ESTABLISHED     5920
  TCP    192.168.100.206:49729  35.190.56.82:443       ESTABLISHED     5920
  TCP    192.168.100.206:49730  104.17.107.108:443     ESTABLISHED     5920
  TCP    192.168.100.206:49770  35.190.56.82:443       ESTABLISHED     1908
  TCP    192.168.100.206:49773  104.17.108.108:443     ESTABLISHED     6200
  TCP    192.168.100.206:49776  35.190.56.82:443       ESTABLISHED     1908
  TCP    192.168.100.206:49778  104.17.107.108:443     ESTABLISHED     1908
```

```
C:\Windows\system32>tasklist

Nombre de imagen                PID Nombre de sesión Núm. de ses Uso de memor
========================= ======== ================ =========== ============
System Idle Process               0 Services                   0          8 KB
System                            4 Services                   0        148 KB
Registry                         92 Services                   0     76.896 KB
smss.exe                        576 Services                   0        960 KB
csrss.exe                       700 Services                   0      5.344 KB
wininit.exe                     772 Services                   0      6.848 KB
csrss.exe                       780 Console                    1      5.596 KB
winlogon.exe                    868 Console                    1     11.112 KB
services.exe                    888 Services                   0      9.180 KB
lsass.exe                       920 Services                   0     20.936 KB
svchost.exe                     328 Services                   0     32.452 KB
fontdrvhost.exe                 624 Console                    1      6.156 KB
fontdrvhost.exe                 644 Services                   0      3.448 KB
svchost.exe                    1052 Services                   0     14.736 KB
svchost.exe                    1104 Services                   0     10.148 KB
dwm.exe                        1180 Console                    1     86.472 KB
svchost.exe                    1280 Services                   0      5.248 KB
svchost.exe                    1300 Services                   0      6.016 KB
svchost.exe                    1364 Services                   0     10.064 KB
svchost.exe                    1376 Services                   0     12.220 KB
svchost.exe                    1516 Services                   0     15.940 KB
svchost.exe                    1532 Services                   0     22.408 KB
svchost.exe                    1548 Services                   0      6.952 KB
svchost.exe                    1564 Services                   0     11.904 KB
svchost.exe                    1644 Services                   0      6.660 KB
svchost.exe                    1692 Services                   0     10.120 KB
svchost.exe                    1724 Services                   0      6.944 KB
svchost.exe                    1836 Services                   0     11.676 KB
bdservicehost.exe              1888 Services                   0     20.276 KB
bdservicehost.exe              1908 Services                   0    261.392 KB
svchost.exe                    1100 Services                   0      9.660 KB
VBoxService.exe                2204 Services                   0      6.468 KB
bdservicehost.exe              2324 Services                   0     49.952 KB
bdservicehost.exe              2336 Services                   0     29.620 KB
wsc_proxy.exe                  2588 Services                   0     12.040 KB
```



Windows Update

¡Todo está actualizado!
Última comprobación: hoy, 13:12

Buscar actualizaciones

Seguridad de un vistazo

Consulta lo que está sucediendo con la seguridad y el estado del dispositivo, y toma las medidas necesarias.

Protección contra virus y amenazas
Estado no disponible, abre Bitdefender Antivirus para obtener más información.
Abrir Bitdefender Antivirus

Protección de cuentas
No se requiere ninguna acción.

Firewall y protección de red
No se requiere ninguna acción.

Control de aplicaciones y explorador
No se requiere ninguna acción.

Seguridad del dispositivo
Ver el estado y administrar las características de seguridad de hardware

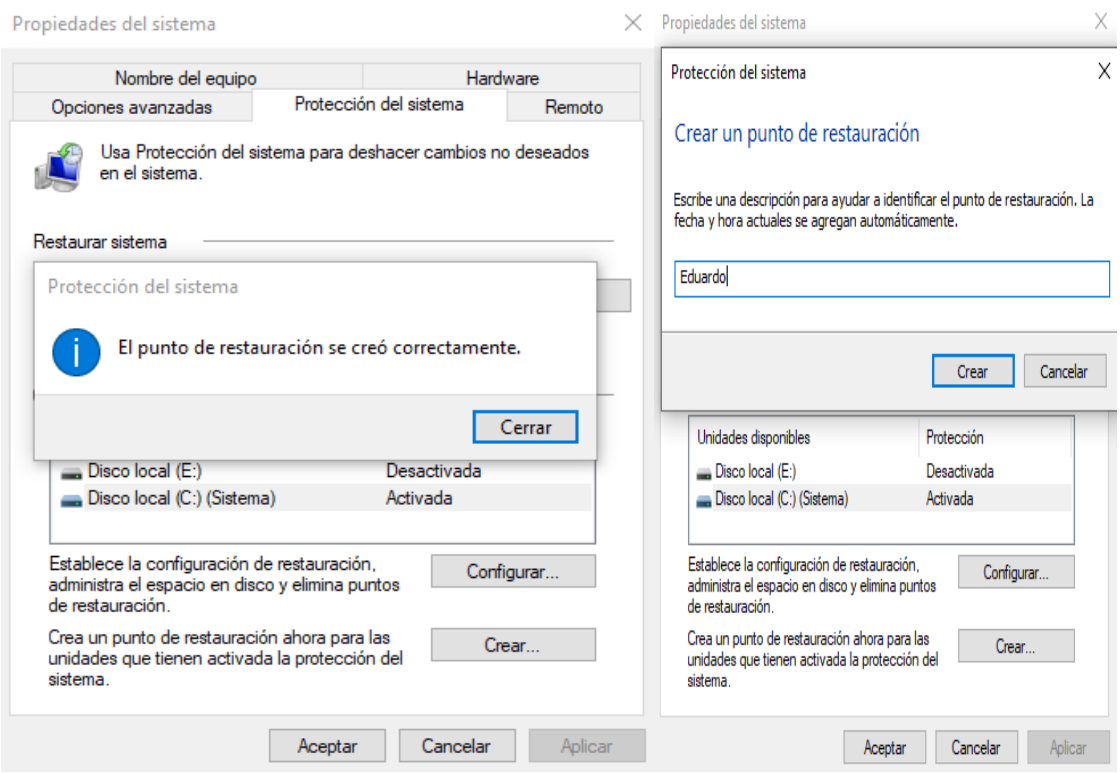
Rendimiento y estado del dispositivo
No se requiere ninguna acción.

Respaldo y Recuperación

Para asegurar la estabilidad del sistema antes de aplicar cambios, se creó un punto de restauración en Windows. Esto permite regresar el sistema a un estado previo en caso de problemas posteriores.

Creación del Punto de Restauración

Se utilizó la herramienta de Protección del Sistema para crear un punto de restauración manualmente. El proceso fue sencillo y tardó aproximadamente **3 minutos** en completarse. Se verificó que el punto estuviera disponible para futuras restauraciones.

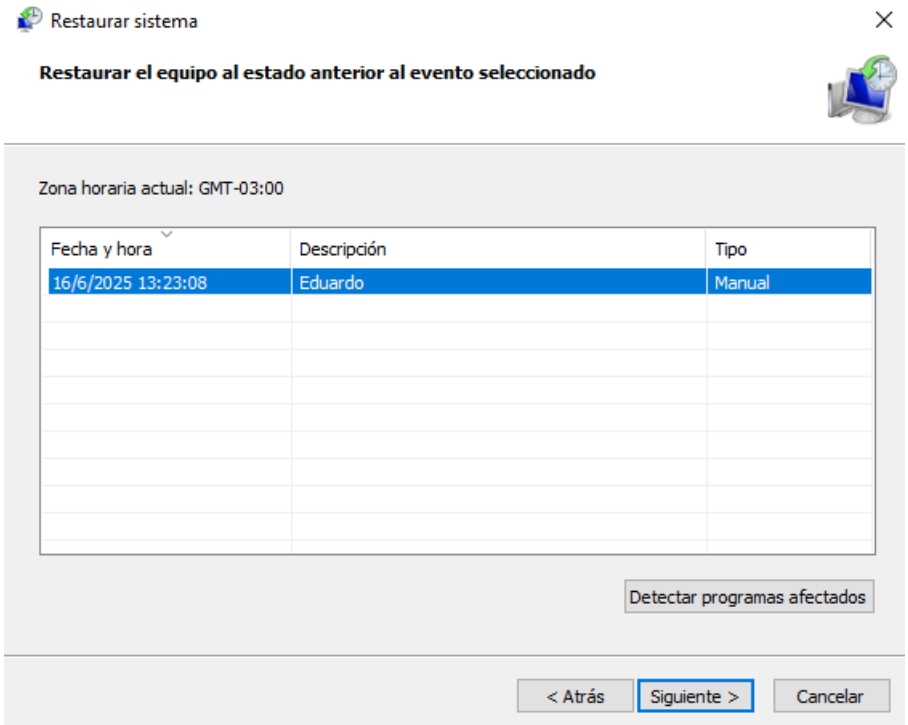


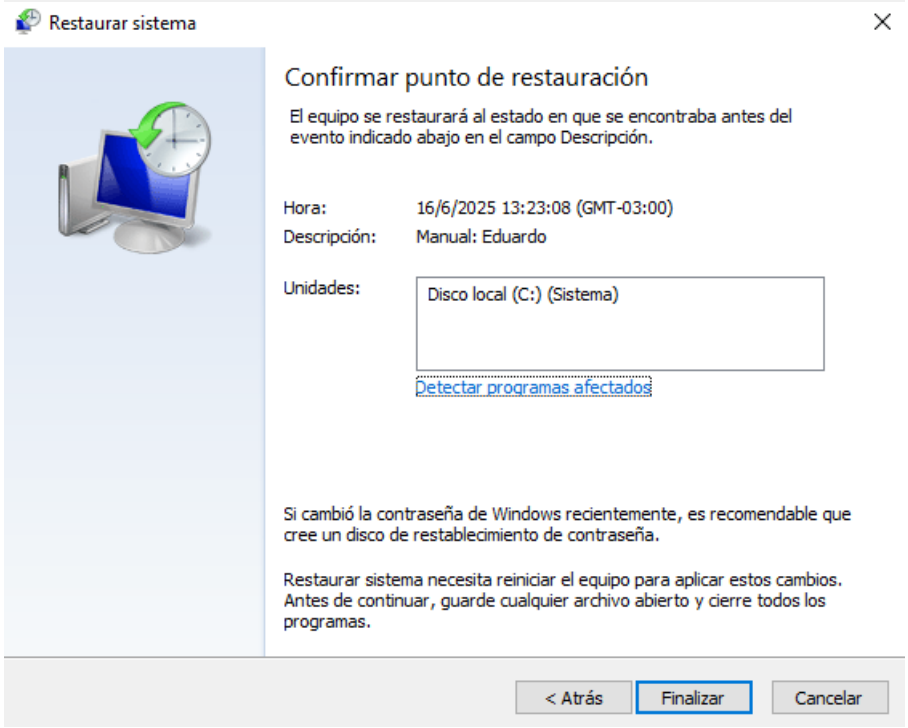
Realización de Cambios al Sistema

Tras crear el punto de restauración, se desactivaron varios servicios considerados innecesarios, como los servicios de telefonía y WalletService, con el objetivo de optimizar el rendimiento y seguridad del equipo.

Restauración y Verificación

Se realizó una restauración del sistema al punto creado previamente para comprobar que el proceso funcionara correctamente. La restauración se completó exitosamente en aproximadamente **5 minutos**, y el sistema volvió a su configuración original sin pérdida de datos.





Documentación del Proceso y Tiempo

- Tiempo de creación del punto de restauración: **3 minutos**
- Tiempo para realizar los cambios en servicios: **7 minutos**
- Tiempo de restauración del sistema: **5 minutos**

Este proceso es fundamental para mantener la integridad del sistema, permitiendo revertir cambios que puedan afectar negativamente su funcionamiento o seguridad.

Conclusión

A lo largo del desarrollo del Laboratorio 4 se realizaron prácticas fundamentales orientadas a fortalecer la seguridad del sistema operativo Windows. En la sección de auditoría, se activaron los registros de eventos de seguridad y se ejecutaron acciones específicas que permitieron observar el funcionamiento del sistema ante intentos de acceso no autorizados. El análisis de los logs evidenció que el sistema genera trazas claras y detalladas, útiles para la detección de incidentes.

En cuanto al análisis de vulnerabilidades, se identificaron múltiples servicios activos que no son esenciales para el entorno de uso, como servicios de telefonía, WalletService y otros relacionados con conectividad innecesaria, los cuales fueron deshabilitados para reducir la superficie de ataque. También se verificó que el sistema contaba con todas las actualizaciones de seguridad disponibles, manteniendo así una postura preventiva frente a vulnerabilidades conocidas.

Finalmente, en la parte de respaldo y recuperación, se comprobó la efectividad de los puntos de restauración del sistema. Se creó uno antes de realizar cambios y posteriormente se revirtió el estado del equipo sin pérdida de información, validando la utilidad de esta herramienta ante modificaciones o fallas inesperadas.

En resumen, el laboratorio permitió poner en práctica herramientas reales de protección, auditoría y recuperación del sistema, reforzando el conocimiento práctico sobre los mecanismos de defensa del sistema operativo Windows y la importancia de una configuración segura y controlada.